Privacy Actors, Performances and the Future of Privacy Protection

Chapter 12
Privacy Actors, Performances and the Future of Privacy Protection

Charles Raab and Bert-Jaap Koops

12.1 Background

A large proportion of the scholarly work on privacy and data protection has focused attention on the instruments or 'tools' that are, or that could be, used for regulating the processing and flow of personal data. This important research has generated considerable debate, criticism and (re)conceptualisation of the means whereby rights or claims to privacy can be defended or promoted. Much of the discourse around data protection has had to do with the merits or shortcomings of laws, directives, codes of practice, privacy statements and seals, privacy-enhancing technologies (PETs), contracts, binding corporate rules, international agreements and treaties and so on (e.g., Bennett and Raab, 2006).

Discussions of the instruments are sometimes partisan, reflecting, for example, preferences for or against state control and pressures for self-regulation or for technological solutions. This should serve to remind us that designing the instruments that are the 'how' of data protection is not a dispassionate technocratic process of choosing tools to do a job but a political process in which there are many conflicts and interests, in which more than data protection is at stake. In particular, the merits of, and relationship between, legal instruments and system architecture or 'code' has held centre-stage as a principal topic of analysis (Lessig, 1999). The emphasis on some instruments (e.g., self-regulatory codes of practice), which was strong in American policy discourse, has faded somewhat from prominence in the debates of the new century, although market-based or property solutions retain their vigour to a large extent, in part reflecting frustration with the difficulty of regulating privacy through supra-individual institutional processes in a global information environment.

The value of tools-oriented analysis is that it helps to clarify the 'how' and 'what' of information privacy protection and perhaps also the 'what works?' orientation of policy-makers and practitioners. The expected further development of information

C. Raab (✉)
School of Social and Political Science, University of Edinburgh, Edinburgh, Scotland, UK
e-mail: c.d.raab@ed.ac.uk

Bert-Jaap Koops wrote this paper as part of a project on law, technology and balances of power that was funded by NWO, the Dutch Organisation for Scientific Research.

S. Gutwirth et al. (eds.), *Reinventing Data Protection?*
DOI 10.1007/978-1-4020-9498-9_12, © Springer Science+Business Media B.V. 2009

and communication technologies (ICTs), as well as innovations in the application of ICTs in economic production and consumption, in public administration and in law enforcement and public order domains, are likely to bring forth new regulatory instruments or new variations on older ones. No doubt, these will keep the scholarly industry alive. Although the pursuit of understanding in terms of regulatory instrumentation is far from exhausted, we need to know more about the array of instruments *as an ensemble*, or how each one functions as a component of a holistic regulatory regime, both descriptively and in terms of possible improvements in regulatory design (Bennett and Raab, 2006; Raab and De Hert, 2007, 2008).

But whilst further exploration of this is necessary, it is insufficient for achieving the aim of understanding regulation without bringing in a further dimension of the analytical paradigm: the 'who' of privacy protection, considering both who are the protectors and who are the protected. Moreover, just as we cannot understand tools without seeing them in relation to each other, we cannot understand these actors without understanding *action*; that is, the relationships and processes through which actors come together in co-operation or conflict, whether to shape the tools, use them, or avoid them. Regulators and other practitioners may understand these dimensions very well and no doubt have well-developed views on who *ought to* take part in the process, when and where.

If we are to point to the future, it may well be important to look a bit more systematically at these dimensions, in order to see how improvements could be made in the existing processes of decision-making, the patterns of responsibility and accountability and the relationships amongst participants. It is arguable that the problems of data protection, as well as the successes, are attributable in considerable part to the participants or policy actors, to the roles they play and to the institutions in which action takes place and not only to the instruments or tools that are used to protect personal data. The focus of attention here is therefore on the policy actors and the institutions they inhabit. It is also concerned with where these actors and institutions are located in 'policy space', which comprises the governmental or political arenas that exist within particular jurisdictions and at different levels from the local to the global. We might say that that is the 'where' of privacy protection. Moreover, because these relationships take place in real time, there is also a question about 'when', which points up the element of 'process' more than just an account of actors who do certain things. Whether it is the 'what', the 'who', the 'where' or the 'when' of regulation that is under investigation, we should not lose sight of the *exercise of power* as a crucial dimension of these phenomena. This points towards other, more normative, aims of this paper: to consider the responsibilities of actors and to evaluate performances, even if only in broad-brush terms, in order to show the way to possible changes.

12.2 Mapping the Landscape of Actors

In regard both to instruments and levels or arenas, there is a very disjointed landscape that defies simple description or the easy reading of trends. This paper cannot provide a comprehensive account of the expanding policy community for privacy

and data protection but the available evidence is of a complex patterning of a highly diverse and shifting array of groups, networks and other comings-together, some more institutionalised than others, that have barely emerged as the subject of contemporary systematic research. There may be a prospect of effective global regulation or, on the other hand, an increasing incapability of existing and foreseeable instruments and regulatory strategies. There is a range in-between these poles, in which path-dependent patchworks of *ad hoc* tools, organisations and strategies cope with problems, with some, but limited, success. These reflect the generations of privacy protection from the 1970s to the present and thus encompass the historic responses to major technological change, as well as accommodations or resistances to privacy-unfriendly political and commercial initiatives.

It is now some 39 years since the establishment of the first regime for the protection of personal data, that of the German *Land* of Hesse, which included a regulatory agency headed by a privacy commissioner (Bennett, 1992). Since then, there has been a proliferation of such organisations and officials across the world, in individual countries and in smaller jurisdictions (i.e., within federal countries). The history of developments in these jurisdictions need not be rehearsed here; nor does the way each such regime has mixed and matched particular instruments according to its own politically-driven estimate of the relative value of laws, codes of practice, technological instruments and other tools or mechanisms in protecting information privacy (see Bennett and Raab, 2006). These policy 'choices' have often been driven by international legal requirements, policy learning and borrowing, regulatory traditions and other pressures, as well as, perhaps, chance.

In the present context, it is more important to note that regulatory policies and legislation have taken place at several *levels*, or jurisdictional arenas, which are substantially, albeit disjointedly, interrelated. Early on, information privacy protection became a 'project' of an international informal group of prominent public officials and academics in the 1970s and continued with a further concretisation of rules, principles and guidelines established by institutions, notably the Council of Europe and the Organisation for Economic Co-operation and Development in 1980–1981. These rules and principles shaped subsequent national and sub-national legislation and continued into the second generation when national laws were aligned with a further trans-national landmark in privacy protection, the European Union (EU) Directive 95/46/EC in 1995, itself influenced by national practices and legal provisions. These activities and rules have borne not only upon national jurisdictions but upon sub-national ones as well and on the activities of the private (or at least, non-state) sector of the economy in which personal data are processed. They, and perhaps especially in recent years, the EU, have impinged upon many old members of the club of information privacy regulation, such as the USA and Canada and on many new entrants when they set up their laws and regulatory machinery for the first time, such as the countries of Eastern and Central Europe and the non-Commonwealth countries of the Pacific Rim.

As has just been indicated, there are prominent players in arenas above that of the individual country: international formal organisations have been important from early days onward and have generated some of the main international, authoritative documents having regulatory force. These have helped to set the parameters for

regulation, the understandings of privacy-related issues and the very means of regulation themselves. But new players among international organizations have come along. At the global level, the World Trade Organization (WTO) has played a part in shaping privacy protection in a context of international trade policy. The United Nations, although not a new player, has also lent its moral force to the cause of privacy protection, although it has played little part in practical activity. Regionally, the Asia-Pacific Economic Co-operation (APEC) group of countries have formed regular relationships concerning information privacy protection, from which the APEC privacy framework, albeit much criticised, has been a tangible outcome. In addition, international organisations of other provenances have come into view as participants: global and European standardisation organisations are among the prominent participants, although movement towards the development of world-wide privacy standards has been halting. The movement for the creation of a privacy standard has had its manifestations at national (e.g., Canada), European (CEN/ISSS) and broader international (ISO) levels. Particularly in the ICT context, organisations like the World Wide Web Consortium (W3C) have also aimed at developing privacy standards, such as the Platform for Privacy Preferences (P3P), although the degree of success has not been very high.

Other international mechanisms fall somewhere between formal organisations and networks; or rather, the same members operate in both kinds for different purposes. It is in this context that account must be taken, not only of who does what at what level but at the *interaction* of players across levels as they shape policy and regulatory instruments. Under the European Data Protection Directive 95/46/EC, the so-called Article 29 Working Party has been very prominent on the regulatory landscape in the past decade. As a body that includes representatives of the EU Member States' supervisory authorities, it has produced many reports, opinions and other relevant documents concerning a host of technological, policy and information practice-related issues and operates in relation to other EU institutions. This is also the place to note the formal establishment of the role and office of the European Data Protection Supervisor (EDPS) within the EU, thus underlining the importance of the European level of data protection activity and pointing towards an EU spokesperson role vis-à-vis the rest of the world.

The most visible and long-standing network of wide extent, going back some thirty years, is the circle of the *world's privacy commissioners* that has met annually to compare experiences, to examine regulatory and technological developments and to respond to (or perhaps procrastinate in the face of) immediate issues. This is the maximal grouping, so far, for global regulation of privacy-invasive information practices and of surveillance but it has yet to achieve an organisational presence that persists from year to year. This perhaps exemplifies and signifies the general inhibitions on the formation of global regulation and, in this example, the effect of financial and organisational resource limitations, as well as national political and legislative constraints upon the further development of commissioners' roles. Particularly among some national commissions, it may also reflect a certain reluctance to promote further institutionalisation and the pressures of collective decision-making that such institutionalisation would entail. Over the years, in fact, the annual

commissioners' conference, held in different places across the globe, has produced final communiqués and resolutions but often with apparent difficulty in concerting views on issues of the day that affect the working of all in their national contexts, or in agreeing on the very propriety of such concertation.

Just what the difficulties here have been, what explains them, and the perceived prospects for overcoming them as international data protection moves into a future marked by increasing surveillance-related threats to the privacy that the regimes have been constructed to protect, should be among the main subjects of future policy-oriented research. There are, however, some signs that this network may become more institutionalised and bureaucratised, possibly spawning its own secretariat and thus potentially operating in a more visible and regular way between the annual occasions that have been hitherto organised on a rotating *ad hoc* basis. There may possibly be a pay-off in terms of greater influence, or at least voice, in the world's arenas where policies are made that pose threats to privacy. These include a number of data-gathering and surveillance activities that have proliferated at least since the events of 11 September 2001 and that have put privacy protection on the defensive (see, e.g., EPIC, 2006).

Within its orbit but not organisationally connected to it are smaller groupings or networks of regulators taking a special interest in, for example, the field of telecommunication and its privacy implications. There are also gatherings of European privacy commissioners (or similar titles) in larger or smaller groupings for mutual learning and comparing experiences, based on regional, historic or other affinities. These interactions include those of EU Member States, of the EEA and of sub-jurisdictions in Germany, Switzerland and Spain, as well as of Jersey, Guernsey, Cyprus, Malta and the Isle of Man; the expansion of the EU to include new Member States in East and Central Europe has further ramified these patterns of interaction. The first European Congress on Data Protection was held in March, 2006 in Madrid. At the level of EU and European or world-level institutions, there are many other comings-together of commissioners for various purposes: besides the activities of the Article 29 Working Party, important data-protection work is conducted within Europol, Eurojust and Interpol. In all these processes and contexts there have been many other participants apart from information or privacy commissioners but the latter have been the most identifiable category or grouping, with some degree of continuity and coherence manifested through their networks and more formal arrangements.

Thus, during the decades in question, there have been increasing efforts to create roles, networks and organisations of regulatory bodies and individual actors across jurisdictional lines, with a particular concentration within Europe but with important intercontinental linkages as well. There are also significant affinities and interchange among agencies within particular linguistic groupings in the Francophonic and Spanish-speaking worlds. Networks and ad hoc concentrations of a more specialised sort have also been evident in domains in which privacy issues are prominent in relation to new ICT (e.g., telecommunications; radio frequency identification (RFID)) or other developments in the fields of business and government. Taken together, these and other formal or less formal arrangements beyond the national state resemble

a *kaleidoscope*, in which the same pieces group and regroup periodically in the course of time; the 'usual suspects' have the chance to come together frequently in the rounds of meetings and other means of communication they use for dialogue, deliberation and common action. Some of this club-like behaviour is carried out publicly and transparently and the network boundaries are fairly penetrable by other persons, who may work in privacy-related roles in other public bodies, private-sector companies, academia and interest groups and who have relatively easy access to some meetings and to the members of the 'club'. We may note, also, the emergence of international gatherings of the world's freedom-of-information commissioners, in ways that resemble their privacy counterparts; in some cases, these may be the same persons (or at least the same regulatory authorities) wearing different hats.

Beyond those developments of the past few decades and of very recent years, new roles and, indeed, careers and formal qualifications have proliferated in a host of organisations such as firms and public agencies. These include data protection or privacy officers, chief information officers and the like, who are charged with responsibility for the legal compliance and good practice of their organisations and who have developed institutional bases for their training, common learning, interest co-ordination and representation. Their activities emanate from organisations, both private and public, within countries and among prominent multinational firms and represent a movement towards professionalism as well as policy interest and collective representation. There are now many thousand such persons on the scene; many of them also intersect with, or even double up as, the officials responsible (in some countries) for compliance with freedom-of-information in their organisations, given the close relationship between, and even mutual entailment of, these two aspects of information policy.

Further afield in the regulatory universe are the groupings of privacy advocates in and among a number of countries, such as the Electronic Privacy Information Center (EPIC) and Privacy International, whose members and spokespersons play significant parts in pressure-group and advisory activities that flow into the shaping of regulation.[1] They have well-publicised, regular conferences and meetings (e.g., the annual Computers, Freedom and Privacy conference) and host active websites, e-mail discussion and information networks and blogs. Of particular interest is the European combination of national privacy-advocate organisations, European Digital Rights (EDRI), founded in 2002 by a few national groups and now boasting 29 privacy and civil-rights groups in 18 European countries, resulting in a significant increase in sharing and spreading information on impending surveillance and privacy-threatening measures, if not necessarily in lobbying power, as many of the constituent groups operate largely independently at their own national levels. These privacy groups overlap with a host of citizens', consumers' and human rights bodies that act nationally, regionally or internationally, often concerting views and activities across national boundaries and attempting to influence policies at several levels. Counterposed to those, of course, are groups and networks that seek to *limit* privacy

[1] Systematic research on privacy advocates is reported in Bennett (2008).

protection by shaping regulatory rules or instruments in ways that, they believe, will properly minimise the impediments to the commercial or state activities that make extensive or intensive use of personal data. Yet there are signs that, among these mainly industrial and commercial interests, privacy and data protection are coming to be seen as 'good business' and therefore as something to be accommodated and shaped rather than resisted. Understanding all these actors' relationships with others in policy space and the policy-process dynamics in which they are engaged is especially important for an analytic framework that incorporates conflict and negotiation as major processes and that does not necessarily seek to tell stories either about the onward march of privacy protection or the inevitable erosion of privacy.

12.3 The 3D-Landscape: Multi-Level Governance?

Thus, since the inception of privacy protection as a felt responsibility of states in regard to their citizens and inhabitants, we have been witnessing the development of a rich but variegated pattern of connections of a variety of frequencies and densities in and around the issues, instrumentation and practices of privacy protection. The *effectiveness* of this regulatory activity is a crucial but different question that defies attempts at measurement and evaluation, as Bennett and Raab (2006) have argued. Be that as it may, it is nonetheless appropriate to consider how far this phenomenon constitutes, or promotes, the institutionalisation of a multi-level governance (MLG) infrastructure (Bache and Flinders, 2004; Hooghe and Marks, 2003) to regulate information practices in line with a framework of laws, human rights and other principles that aim at the control of surveillance (defined broadly) and the protection of privacy. To the extent that the politics of privacy protection is becoming the *international relations* of privacy protection, it is open to question what the relevant analytical frameworks or 'theories' may be for investigating them. MLG seems to bridge the politics and the international relations but only systematic study would show its usefulness or its need for modification, or perhaps rejection, for the purpose of understanding information-policy regimes such as that for the protection of privacy or personal data.

If one is talking about groups, networks, roles, circles, clubs, bodies and so on, one is not necessarily talking about discrete *levels* in a jurisdictional or geographical sense, although those levels are important as targets or sources of regulatory activity and many of the policy actors can be located at one level or another. Although the meaning of 'level' is far from clear in the relevant theoretical literature, 'levels' as a term referring to place or jurisdiction is, in any case, too tidy a concept to embrace activity that is so scattered in time and space and that takes place in ways that do not conform to the nesting, hierarchical and sometimes inter*governmental*-relations implications of MLG approaches. But these implications are not intrinsic to such approaches, although there may be some important hierarchical arrangements within a looser set of relationships and these may properly attract the label 'multi-level': for example, the formal relationship between institutions of the EU and those of

the Member States is such that, in the privacy field, EU Directives are binding on national governments and are supposed to generate compliant activity at that level and within it.

Nor is it to be assumed that MLG involves only *public-sector* actors or organisations. This is because one of the characteristics of 'governance' *tout court* is the involvement of a mixture – obviously different in specifics within different fields – of policy participants of varied provenance. One of the consequences of the shift from the study of government to the study of governance is that – corresponding to the complexity of the world – there is little collective or individual behaviour that can be ruled out, *a priori*, as candidates for inclusion in accounts of the policy processes for the particular subject at hand, whether it is the health or education services, transport, public order – or information privacy. The involvement of standardisation bodies, technology and retail firms, or activist groups in the shaping of regulation in the privacy field are examples of this. Other examples of a more traditional kind can be found in the privacy-related activities of individual firms nesting within the framework of similar activity undertaken at a higher level for an industry as a whole, such as a sectoral trade association (e.g., a direct-marketing association), although the efficacy of such self-regulation through, for example, private-sector industrial codes of practice, at and between private-sector levels, arouses scepticism. In any case, the 'governance' part of MLG betokens a vast research endeavour, not only to 'name the parts' that are involved but to comprehend their relationships and contributions toward producing a regulatory output and outcome. As with the study of governance in other fields and also more generally, the risk of losing sight of the contribution and sometimes the pre-eminence, of central states is ever-present, especially if one were to adopt the unsustainable position that the Internet, for example, is ungovernable, not least by state activity.

12.4 How Does the Landscape Function?

An important next step in analysis is to look more closely at policy actors and at their different roles. By looking at the various roles and responsibilities that all policy actors are given or take on themselves, we can assess any gaps in the distribution of all aspects of privacy protection across the range of actors. Table 12.1 attempts this in a generalised and basic fashion[2]:

This table does not necessarily imply that there is a strict one-to-one relationship between actors and roles, nor can it show that, for the most part, there are complex interdependencies amongst actors, just as there are for policy instruments or tools. A more elaborate – multi-dimensional – table, including a time dimension, would be necessary for a realistic picture of these relationships that would show how

[2] Bennett and Raab (2006: 220) draw an analogous diagram of actors but do not explicitly indicate their roles.

Table 12.1 Actors and their privacy roles and responsibilities

Actor	Responsibility
Constitution-maker	Stipulate the right to privacy
Legislature	Make privacy-compliant laws and data protection acts
Data protection authority	Supervise and enforce compliance, encourage good practice, raise awareness in public and politics
Court	Decide cases involving privacy breaches
Government department or agency	Compliance, staff training in privacy protection
Private company	Compliance, staff training in privacy protection
Privacy activist organisation	Campaign for privacy, propose regulations, raise public awareness
Academic	Explain privacy and data protection, discern long-term developments
Journalist	Highlight issues and events, explain policies and developments
Consumer	Protect own privacy, complain
Citizen	Protect own privacy, complain
Technology developer	Implement privacy-enhancing technologies (PETs), educate IT professional staff about privacy

role-performance, for any actor, is a collaborative project. However, that is beyond the scope of this paper.

What interests us now is a broad-brush and general assessment of actors' actual performance. A brief roll-call of the actors and how they perform their roles and handle their responsibilities seems to suggest a fairly bleak picture. However, we must start with a *caveat* about any such judgments. As Bennett and Raab (2006: Chapter 9) note, the evaluation of data protection systems is no mean undertaking and is fraught with problems of conceptualisation, criteria, evidence and measurement. As they argue, '[s]ummary statements about effectiveness owe more to the discourse of engaged policy debate and advocacy than to that of reasonably detached analysis' (Bennett and Raab, 2006: 235). Therefore, the judgments made in this paper should not be taken as arising from a base of systematic, intensive and extensive research, which we cannot pretend to have; nor can we say that it exists anywhere. Moreover, they are not tied to any specific country or data protection regime. Judgments will also depend on the criteria or benchmarks that are chosen; these are controversial and not universally established, and it is questionable how far they could be applied fairly to countries and privacy regimes that reflect a great variety of histories, cultures, institutional structures and values. Therefore, the remarks in this paper are indicative best-guesses, sometimes reflecting what can be taken to be conventional wisdom, which may stimulate not only debate but further comparative research in depth. That said, what does the roll-call indicate?

First, constitution-makers have generally created a good basis for privacy protection by including privacy in the constitutional make-up of most national and international legal systems. However, it should be noted that the exceptional grounds for infringing privacy are quite broadly formulated, or at least can be interpreted quite broadly by the courts, as in the case of Article 8 of the European Convention

on Human Rights (ECHR), so that the actual privacy protection at the constitutional level is not very solidly rooted. Perhaps that is inevitable, as the prevailing doctrine is that privacy often needs to be balanced against a variety of competing rights, so that it needs to be flexibly formulated at the constitutional level.

Be that as it may, the result is that at the level of legislatures, both national and supranational (EU), many laws are drafted that are, even if compliant with a constitution, distinctly privacy-unfriendly. The trend in many Western countries, already visible in the 1990s and reinforced after 9/11, is that legislatures, in a piecemeal fashion, consider privacy less important when deciding upon some anti-terrorist, anti-crime, or public-service measure. Legislators seem to pay less attention to, and have increasingly less patience for, the needs of privacy protection, as compared to two or three decades ago. On the other hand, a large number of countries throughout the world have passed significant data protection laws over the past decades and legislatures seem to take their responsibility seriously to create a firm legal basis for data protection in the national and supranational legal systems. One might debate whether the actual form of the resulting data protection legislation, which varies across countries to a significant degree within the framework of universally respected principles, is actually the most suitable for data protection, but that is a different issue. On balance, however, the net effect of privacy-unfriendly and of data protection laws seems to us to be fairly limited from the perspective of privacy protection: with considerable simplification, legislatures currently tend to attack rather than protect privacy in legislation and it is not difficult for them to follow populist and media demands to erode privacy in favour of, for example, security and law enforcement purposes. Yet we should also acknowledge the argument that even the 'best' data protection and privacy laws are weak instruments to regulate technological changes that have privacy implications, sophisticated commercial uses of personal data, government policy imperatives, and – perhaps especially – the Internet and global information flows (Koops and Leenes, 2005).

Let us move on to consider data protection authorities (DPAs) or privacy commissions. As we described above, they are very active on many fronts, including in overlapping cross-border networks and appear to work conscientiously to fulfil their responsibilities. Having said that, one must also be critical of the DPAs' actual effect on privacy protection, although the fault for this may lie elsewhere, in the legislation that established their roles, responsibilities, powers and resources. Thus many DPAs are understaffed, have too few financial and staff resources and sometimes too few powers to be able adequately to supervise and enforce compliance with data protection legislation. Moreover, while some DPAs focus more on supervision, others tend to pay more attention to awareness-raising and lobbying and within the EU, there seem to be some differences in opinion between the various DPAs on crucial issues like transfer of Passenger Name Record data to the USA. This diversity does not seem to enhance the power of the privacy supervisors in Europe – or elsewhere – when it comes to influencing heavily politicised regulatory measures such as the ones we mentioned. So, although DPAs are diligent, they face a difficult job in meeting their heavy responsibility for supervising privacy compliance and for influencing privacy debates and decision-making processes.

Then, there are the courts. An overall impression is that the courts are not acting as a significant or consistent protector of privacy. Partly, of course, this is caused by the quite lenient laws that some legislatures have passed but it is also in part owing to the infrequency of privacy-infringement cases coming before the courts. But the latter argument may also be reversed: as long as the courts do not clearly and seriously punish privacy infringements – and to our knowledge, there are actually few cases in which a privacy breach led to significant civil or criminal sanctions[3] – citizens and consumers have little occasion to go to the courts if their privacy is violated. We could also point out certain cases where the courts have done privacy a distinct disservice; for example, *Khan* v. *United Kingdom*[4] and the European Court of Justice's Passenger Name Record judgment[5] but perhaps these are equally exceptional as cases that substantially punish privacy violators (cf. Bygrave, 2002 for an overview of data protection decisions).

The next category of actors includes public and private organisations that use personal data. Are they as privacy-compliant as they should be and do they sufficiently train their staff in privacy protection? On the whole, although these questions, as with all others, require a depth of empirical research that is not readily available, many would adopt a lenient stance and say that organisations are not doing a bad job when it comes to being privacy-compliant, although almost any except the most scrupulous organisation is bound to violate a few data protection rules. They would argue that shortcomings should probably be blamed more on the extreme complexity, vagueness and the absurdity of certain data protection rules in real-life situations, than on the willingness or effort of organisations to protect personal data. However, there are exceptions to this sanguine picture: in Europe, these might be found perhaps somewhat more in the public than in the private sector, with certain ministries and surveillance agencies consistently downplaying the importance of privacy and data protection. In the United States, it is arguably in the private sector that the most notorious privacy violators are to be found, such as certain data brokers and search-engine providers. On the whole, we could be satisfied with the way that most organisations live up to their privacy responsibilities, if it were not the case that the relatively few exceptions are likely to cause a majority of privacy threats that we face today. It should also be considered that a more nuanced evaluation should distinguish between large and small or medium-sized companies, between government agencies of very different kinds (e.g., some are for law enforcement, others are for providing welfare benefits) and between different types of information

[3] With the exception, of course, of physical privacy violations, like rape and burglary; our argument here refers rather to violations of informational privacy.

[4] [2000] ECHR 195 (12 May 2000). In this case, it was decided that a breach of Art. 8 ECHR (privacy) did not need to have consequences for evidence exclusion in light of Art. 6 ECHR (right to a fair trial); the case therefore effectively condones privacy-violating behaviour by police authorities.

[5] ECJ 30 May 2006, C-317/04. In this case, the – privacy-unfriendly – PNR Agreement with the USA (Council Decision 2004/496/EC of 17 May 2004) was annulled on procedural grounds. The result was that a new PNR Agreement was negotiated with the USA, which was even more privacy-unfriendly than the first one.

activity (e.g., simple use of data, or more sophisticated data-mining and profiling) and different kinds of data flow (e.g., used strictly within one organisation, or shared widely across a range of agencies).

We now come to 'third parties': activists, academics and the media. Most activists are indefatigable and imaginative in approaching their tasks seriously, even against heavy opposition and a few examples, such as EPIC, show that privacy groups can actually make a difference in the shaping of privacy policy. However, the effectiveness of organisations such as EPIC seems exceptional: most privacy groups have few resources and are dependent on volunteers and good intentions rather than a solid popular or political basis on which to build a consistent fight for privacy rights.[6] Privacy activists seem particularly important in the current landscape, where privacy is on the defensive against the threats posed by identity measures, DNA databases and technologies for tracking and recording human movement and transactions and needs active and perhaps combatant spokespersons, However, unless they are based in countries like the US that have a tradition of large-scale private charity, they find it difficult to live up to their task in countries where people are reluctant to contribute substantial financial support.

Academics present a rather ambivalent picture. There is a fairly consistent if rather small group of privacy academics around the world who participate in and add to privacy debates and privacy discourse. They are based in legal, technical, philosophical and social scientific disciplines and a number of them go beyond privacy itself to investigate surveillance and the other values that are affected by it. Almost all of them try to explain and keep abreast of developments in privacy and data protection and several try to influence policy by writing opinions and giving expert statements. On the conceptual side, although 40 years of privacy research have provided useful insight into what privacy actually is, what the relationship is between privacy and data protection and why privacy is so important, academics often have difficulty in getting these conceptual insights across to politicians or to the public. This is not to criticise the academics as a group or individually: we know from experience how hard it is to give convincing answers to the questions raised in a language that fits the frame of reference of politicians and the public. But academics should also realise that as long as such convincing answers, in understandable language, remain absent in public and policy debates, privacy is hard to defend in the current climate. In mounting this defence, an additional problem for many academics is that it is easy for politicians and others to point out that empirical findings about public attitudes towards privacy invasions do not always strengthen the case against excessive surveillance. We refer again to this below.

As to the media, the picture is also mixed. They may be part of the solution but they are certainly part of the problem, as privacy invasion by the media into the lives of celebrities as well as 'ordinary' people seems to sell papers and boost ratings.

---

[6] An illustrative example is the Dutch group Bits of Freedom, which for several years was one of the most well-informed and vociferous groups in Europe but which had to be disbanded for lack of funding in 2006.

The popularity of the 'big brother' television series also attests to the profits to be gained from lives lived in a goldfish bowl. With a few exceptions, most media tend to neglect or downplay privacy as an issue, and particularly the tabloid press and popular commercial television broadcasters have a tradition of not taking privacy seriously in the context of policy issues where 'security' is an overriding concern. But the 'quality press' has a somewhat different tradition and seems to have taken up privacy as an issue that is worthy of news and of concern. Over the past year or two, a shift seems to be slowly taking place, from privacy as a culprit in an 'If-you-have-nothing-to-hide, you-have-nothing-to fear' discourse (cf. Solove, 2007) towards privacy as a vulnerable good in a 'surveillance society' discourse. This only occurs in a small part of the media, albeit in some of the more influential ones but it may be a significant development that indicates that some journalists are shouldering their responsibility in noticing and critically describing societal developments, in this case, the threat to privacy of the increasingly surveilled Western society.

What can be said about the privacy bearers themselves: citizens and consumers as 'data subjects'? They are, to a certain extent, responsible for protecting their own privacy – the proverbial closing of the curtains if they want to hide in-house activity. In some ways, quite a number of citizens certainly do protect their privacy as far as it lies in their power to do so. However, most citizens have little notion of the threats to their privacy that current society poses, particularly since privacy is increasingly infringed by covert, complex and distant technological applications of which citizens have little knowledge. Moreover, many of these technologies cannot be blocked by closing curtains – the counter-technologies, if they exist, lie beyond the power (both in terms of awareness and of availability and cost) of most citizens to apply; many of them must be built into the design of technologies in ways that citizens cannot control.

On top of this, citizens in general do not have as high a regard for privacy as they had a few decades ago, for example, in discussions and surveys about 'security versus privacy'. The 'I have nothing to hide' mantra is often heard – and used by politicians to pass privacy-infringing laws – because many citizens seem to think it unproblematic to decrease privacy by measures aimed at solving crimes and preventing terrorism, on the – erroneous – assumption that the measures will be applied to criminals and terrorists but not to themselves, since they are doing nothing wrong (cf. Solove, 2007). They do not realise that the enhanced surveillance measures often target the population at large and scan unsuspected, ordinary citizens for possible 'uncommon' behaviour that matches 'risk profiles'. What holds for persons as citizens applies more or less equally to them as consumers. Perhaps consumers are, generally, even less concerned over privacy than citizens are, since they see immediate benefits of providing personal data to businesses and hardly any threats of abuse of these data, apart from perhaps being pestered by direct marketing, which is hardly threatening to most people. As a result of the relatively low privacy-awareness and privacy appreciation of citizens and consumers and the consequent ease with which they accept infringements, both actual and potential, of their privacy, the protection of privacy as a core value of society is not particularly advanced, and possibly even weakened, by the privacy bearers themselves.

Then, there is the final actor on our stage: the technology developers. It is commonly assumed that they have no responsibility for privacy protection and it is therefore usually considered that they make no effort to make the technology they develop more privacy-friendly, or at least less privacy-threatening. Although academic literature has started to suggest that, in order to keep privacy alive, privacy-enhancing technologies (PETs) must be used (Lessig, 1999), there is a long way to go before this suggestion will be fully listened to and accepted in the community of technology developers. The attempts to develop and market PETs so far have largely been made by privacy activists, lobby groups, DPAs, or other privacy protectors, with the help of technology developers working in commission but there are only infrequent indications that technology industries are aware of a need or value to pay attention to privacy in the development process. Although a 'business case' for privacy protection can be made, such an enlightened approach is not common; nor is privacy protection, apart from data security – which is, of course, highly important – sufficiently incorporated into public procurement processes. As a consequence, most technology that emerges on the market enables privacy infringement much more than privacy protection, since technology tends to facilitate data collection and merging rather than data shielding (Koops and Leenes, 2005).

12.5 Conclusion

We have mapped the landscape of privacy actors, showing a remarkable range of diverse and versatile actors with many potential interconnections and interrelationships. This suggests that privacy is an object of much attention, action and policy-making and there is indeed an impressive range of activities developed by the array of actors. At the same time – although we must repeat our *caveat* that empirical research is lacking here – a roll-call of actors to survey the way in which each responds to and deals with privacy should not make us optimistic that privacy is well protected across the board. Many actors are diligent and make good efforts to protect privacy, although they often face not only resource limitations that limit their success but also public, commercial and political indifference or hostility. Moreover, quite a number of actors seem to pay less attention to privacy than it deserves, perhaps through an underrating or lack of understanding of its value.

Overall, the cast of privacy actors, despite (or perhaps because of?) the many interconnecting and co-operative roads, gives the impression of being too varied and too fragmented to be able to function well. Since there are so many actors, each with her own responsibility, the risk looms large that each individual actor downplays her own responsibility. Pluralism of regulatory activity is one thing but dilution is the other side of the coin, particularly if there is no director to guide the actors. Individual activities are likely to fail to achieve the available synergies without a strategy that cumulates them into a joint performance that achieves its goal.

If privacy is to be adequately protected – and it is vital for society that it is – some shifts may have to be made among the company of players; we only highlight a few here. The actors could do with better direction and a better script, which emphasises

the characteristics of an overall 'play', or regime, beyond the individual characters and their performances. The government is probably the most important actor to take on more responsibility for championing privacy: they can strengthen its presence in policies, provide more funds to privacy-protecting actors, sharpen and orchestrate the implementation of privacy instruments and co-ordinate and facilitate joint policies and activities. In present and foreseeable political circumstances, however, governments are unlikely to be able to perform these regime-sustaining tasks and international or global governance structures are still embryonic and intermittent. A shift is probably also needed in the responsibilities of technology developers: as long as they are able to dismiss privacy as something that 'society' should take care of once their technology emerges on the market, privacy-threatening technologies will continue to be developed, marketed and applied, with few countervailing technologies that can protect privacy. PETs should be taken seriously as a stronghold in the privacy landscape but they can only become a success if privacy awareness and appreciation become ingrained in the minds of technology developers and embedded in business and governmental decisions and requirements. A more privacy-supportive public opinion is also necessary but there are no clear signs of its emergence despite occasional promising fluctuations. In short, there are many challenges that privacy research, policy and practice face and they are likely to keep us busy in the coming years.

References

Bache, I. and Flinders, M. (eds.) (2004) *Multi-level Governance*, Oxford: Oxford University Press.

Bennett, C. (1992) *Regulating Privacy: Data Protection and Public Policy in Europe and The United States*, Ithaca, NY: Cornell University Press.

Bennett, C. (2008), *Privacy Advocates: Resisting the Spread of Surveillance*, Cambridge, MA: MIT Press.

Bennett, C. and Raab, C. (2006) *The Governance of Privacy: Policy Instruments in Global Perspective* (2nd edn.), Cambridge, MA: MIT Press.

Bygrave, L. (2002) *Data Protection Law: Approaching Its Rationale, Logic and Limits*, The Hague/London/New York: Kluwer Law International.

Electronic Privacy Information Center (2006), *Privacy & Human Rights. An International Survey of Privacy Laws and Developments*, EPIC 2006.

Hooghe, L. and Marks, G. (2003), 'Unraveling the Central State, but How? Types of Multi-level Governance', *American Political Science Review*, 97(2): 233–243.

Koops, B.-J. and Leenes, R. (2005), ' "Code" and the Slow Erosion of Privacy', *Michigan Telecommunications & Technology Law Review* 12(1): 115–188, http://www.mttlr.org/voltwelve/koops&leenes.pdf.

Lessig, L. (1999), *Code and Other Laws of Cyberspace*, New York: Basic Books 1999.

Raab, C. and De Hert, P. (2007) 'The Regulation of Technology: Policy Tools and Policy Actors', Tilburg University Legal Studies Working Paper No. 004/2007 (TILT Law & Technology Working Paper Series No. 003/2007).

Raab, C. and De Hert, P. (2008) 'Tools for Technology Regulation: Seeking Analytical Approaches Beyond Lessig and Hood', in Brownsword R. & Yeung K., *Regulating Technologies*, Oxford, Hart Publishers, Oxford: Hart Publishing.

Solove, D. (2007) ' "I've Got Nothing to Hide" and Other Misunderstandings of Privacy', *San Diego Law Review*, 44:745.